NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

REQUIREMENTS FOR THE DEPLOYMENT OF PUBLIC KEY INFRASTRUCTURE (PKI) IN THE USMC TACTICAL ENVIRONMENT

by

Alan R. Stocks

June 2001

Thesis Advisor:	Daniel F. Warren
Associate Advisor:	Cynthia E. Irvine

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2001	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : Requirements for the Deployment of Public Key Infrastructure (PKI) in the Tactical Environment.

5. FUNDING NUMBERS

6. AUTHOR(S)
Stocks, Alan R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

Marine forces are expeditionary in nature yet require the full range of Public Key Infrastructure (PKI) services at deployed sites with limited bandwidth and access to their respective Registration Authority (RA). The development of a PKI solution for the tactical arena is a fluid and complex challenge that needs to be answered in order to ensure the best support of tactically deployed forces. Deployed Marine forces will need the capability to issue and re-issue certificates, perform certificate revocation, and perform key recovery within the command element of the deployed unit. Since the current United States Marine Corps (USMC) PKI was not designed with the tactical environment in mind, the full extent of PKI deficiencies for field operation is unknown. This thesis begins by describing public key cryptography, the implementation and objectives of a USMC PKI, and the components necessary to operate a PKI. Next, tactical issues that have been identified as areas of concern along with their proposed solutions are presented. Supporting material describes design issues, such as scalability and interoperability, and technical challenges, such as certificate revocation lists (CRL), key escrow and management of tokens.

14. SUBJECT TERMS Public Key Infrastructure (PKI), Computer Security, Navy Marine Corps Intranet (NMCI)

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239

Approved for public release; distribution is unlimited

REQIUREMENTS FOR THE DEPLOYMENT OF PUBLIC KEY INFRASTRUCTURE (PKI) IN THE USMC TACTICAL ENVIORNMENT

Alan R. Stocks
Major, United States Marine Corps
M.S., Troy State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2001

Author: _____

Alan R. Stocks

Approved by: _____

Daniel F. Warren, Thesis Advisor

_____

Cynthia E. Irvine, Associate Advisor

_____

Dan C. Boger, Chairman
Information Systems Academic Group

ABSTRACT

Marine forces are expeditionary in nature yet require the full range of Public Key Infrastructure (PKI) services at deployed sites with limited bandwidth and access to their respective Registration Authority (RA). The development of a PKI solution for the tactical arena is a fluid and complex challenge that needs to be answered in order to ensure the best support of tactically deployed forces. Deployed Marine forces will need the capability to issue and re-issue certificates, perform certificate revocation, and perform key recovery within the command element of the deployed unit. Since the current United States Marine Corps (USMC) PKI was not designed with the tactical environment in mind, the full extent of PKI deficiencies for field operation is unknown. This thesis begins by describing public key cryptography, the implementation and objectives of a USMC PKI, and the components necessary to operate a PKI. Next, tactical issues that have been identified as areas of concern along with their proposed solutions are presented. Supporting material describes design issues, such as scalability and interoperability, and technical challenges, such as certificate revocation lists (CRL), key escrow and management of tokens.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like to thank Professor Daniel F. Warren and Dr. Cynthia E. Irvine who shared their time and knowledge in helping me complete this journey. Specifically, I would like to give a special thanks to Professor Daniel F. Warren for his enthusiastic guidance, tutelage, and patience during the completion of this thesis.

Finally my sincerest appreciation, gratitude and admiration go to my wife Jackie, whose patience, love and understanding never faltered during the journey.

I. INTRODUCTION

Throughout history, military leaders have regarded information superiority as a key enabler of victory. The Marine Corps must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority" – better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the Marine Corps to shape the situation or react to changes and accomplish its mission. The Marine Corps of the future will use superior information and knowledge to achieve decision superiority, to support advanced command and control capabilities, and to reach the full potential of dominant maneuver, precision engagement, full dimensional protection, and focused logistics.

Marine forces are expeditionary in nature and require the full range of Public Key Infrastructure (PKI) services at deployed sites with limited bandwidth and access to their respective Registration Authority (RA). Deployed Marine forces will need the capability to issue and re-issue certificates, perform certificate revocation, and perform key recovery within the command element of the deployed unit. In addition, tactical requirements dictate that

provisions must be made to accommodate issuing certificates to allied and coalition forces during combined/coalition operations.

The current plan for the implementation of the United States Marine Corps (USMC) PKI calls for centralized certificate management and decentralized registration. Within this type of architecture, the USMC will issue certificates to all military and Marine civilian personnel by October 2002. However, the tactical environments that the USMC faces present a unique set of challenges to this architectural approach. Since the current United States Marine Corps (USMC) PKI was not designed with the tactical environment in mind, the full extent of PKI deficiencies for field operation is unknown.

To further understand the tactical challenge, one must appreciate the basic definition of tactical. For purposes of this document, tactical is defined as “any environment where networked computers exchange protected information in support of combat operations”.

The nature of the tactical arena invariably suggests that the USMC must employ alternative solutions, at least in part, to institute PKI tactically. It is recognized that injecting PKI into tactical operations will significantly change the way units prepare for deployments. The challenge

arises from the need to alter the architecture to fit the requirements of the tactical arena. Which elements of traditional PKI will be needed within the tactical arena? How will that be accomplished? For example, moving a Certification Authority (CA) away from the centralized region of the current architecture and closer to the Local Registration Authorities (LRAs) will affect the maintenance of secure and stable connectivity with remaining CAs. Hence, the USMC needs to address specific tactical PKI requirements. Based on experience and technical knowledge, the USMC has identified areas of concern, which is the focus of the thesis.

A. THESIS OUTLINE

This thesis begins with a description of the tactical PKI problem. Chapter II introduces public key cryptography which is an emerging technology that supports the cryptographic services of confidentiality, authenticity, integrity and non-repudiation. Public key cryptography differs from conventional cryptography in that two mathematically related, yet different keys are used for encryption and decryption, instead of identical copies of the same key. Where conventional cryptographic services is limited to supporting confidentiality and integrity, public

key cryptography can be used to support confidentiality and integrity, as well as authentication and non-repudiation.

The last section of Chapter II, describes the various aspects of a PKI.

Chapter III describes the USMC PKI implementation. The main six USMC PKI entities are presented in a top down sequence starting with the Root Authority, followed by the Certificate Authority (CA), Registration Authority (RA), Local Registration Authority (LRA), Trusted Agents (TA), and ending with the End-Users. Objectives for the USMC PKI are explained and a current timeline for the implementation and deployment of the USMC PKI is given.

In Chapter IV tactical issues and proposed solutions are identified and described. Tactical issues concerning key escrow/recovery, PKI directory services, and certificate revocation lists are presented. Additional topics include the management of tokens, transportation, biometrics, and a discussion of the loss or capture of personnel and equipment.

Chapter V summarizes the key points of the thesis and presents general conclusions based on the thesis research. The implementation of a tactical PKI within the USMC is a complicated and diverse challenge that requires careful and methodical planning to ensure that tactical forces are

deployed with a workable solution for tactical requirements. Chapter V identifies and briefly discusses additional issues for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PUBLIC KEY CRYPTOGRAPHY AND INFRASTRUCTURES

A. INTRODUCTION

This Chapter introduces public key cryptography as an emerging technology that provides mechanisms supporting confidentiality, authenticity, integrity and non-repudiation, which will be described later. Public key cryptography differs from conventional cryptography in that two mathematically related, yet different keys are used for encryption and decryption, instead of identical copies of the same key. Where conventional cryptography is limited to providing confidentiality and integrity, public key pairs can be used to provide confidentiality and integrity, as well as authentication and non-repudiation. The last section of this Chapter will explain what encompasses a PKI in detail to further understand the technical challenges.

B. CRYPTOGRAPHY

Cryptography means hidden writing, the practice of using encryption to conceal text [Ref 22, p. 23]. Cryptography does for electronic information what locks do for printed information. The information is protected by scrambling it in such a manner that it can be unscrambled only with a secret key [Ref 21, p. 286].

Cryptography has become increasingly important in the last few years. The increased use of networking and the availability of commercial cryptographic products has fueled this increased interest. Years ago cryptography was mainly a national security concern for protecting the confidentiality of classified information.

Recent developments have seen a greater concern for security in the commercial as well as the DoD environment and the additional need for authenticity and integrity have become increasingly important.

Some of the increased interest in the use of cryptography is due to the services that are provided by Public Key Cryptography. Public key cryptography can provide a superior means of authenticating oneself across a network than traditional password protections. Public key cryptography supports digital signatures which are important for communications so that the recipient of a message can be assured that the message really came from the person who claims to be the sender. Digital signatures also provide assurance that the content has not changed since it left the sender. Integrity and authentication of messages have become important within the Defense Message System (DMS) and various other USMC applications. Standards, such as Secure Multipurpose Internet Mail Extension (S/MIME) may stimulate

greater use of secure mail over the Internet, if vendors implement the standard such that interoperability among vendor's secure mail products is achieved.

Encryption and digital signatures are also important for electronic transactions. Encryption can be used to protect SBU data from unauthorized observation and digital signatures can be used to ensure that the claimed individual really is authorizing an order. For the USMC, digital signatures will prove useful in tactical areas by providing assurance of the integrity of a request for resupply, authenticity of the request for resupply, and verification that the request was received.

Conventional cryptography, which has historically been used, provides for confidentiality and integrity. In order to successfully use public key cryptography, certain services such as key generation, key distribution, key revocation, etc. are required. A public key infrastructure of sufficient size and scope to adequately address all USMC needs must be deployed to make use of the technology.

C. PUBLIC KEY CRYPTOGRAHY

Conventional cryptography (also called symmetric-key) and public-key cryptography (also called asymmetric-key) are both based on complex mathematical algorithms and use keys.

Symmetric-key cryptography schemes provide message confidentiality by requiring the sender and receiver to share a common, secret key. Each user must trust the other not to divulge the common key to a third party. These systems encrypt large amounts of data efficiently; however, they pose significant key management problems in networks of more than a very small number of users, and today are typically used in conjunction with public-key cryptography. Examples of this include, electronic commerce by protecting credit card transactions and a variety of ticketing systems from manipulation and fraud.

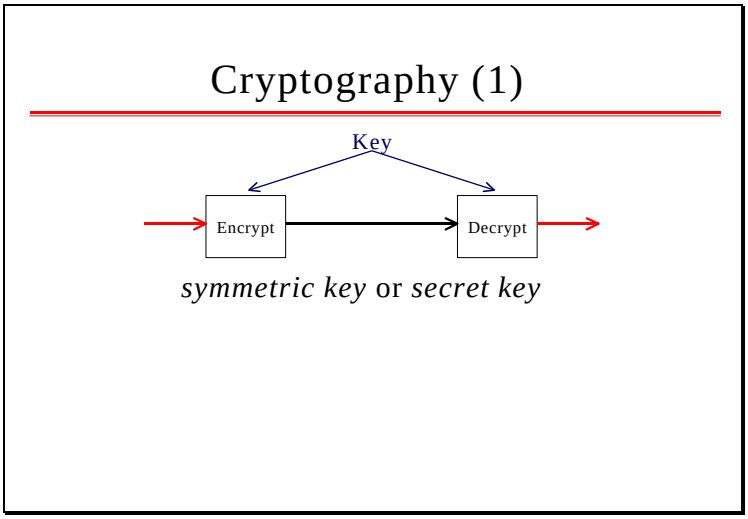

Figure 1. Symmetric Key Cryptography

In 1976, two cryptographers at Stanford University, Whitfield Diffie and Professor Martin Hellman, invented a

method whereby two parties could agree on a secret message key without the need for a third party, an off-line exchange, or transmission of any secret values [Ref 21, p. 298]. The Diffie-Hellman method is based on the concept of a private-public key pair.

Public-key cryptography schemes require each party to have a key pair: a private key, which must not be disclosed to another user, and a public key, which may be made available in a public directory. The two keys are related by a hard one-way function, so it is computationally infeasible to determine the private key from the public key. Since the security of the private key is critical to the security of the cryptosystem, the private key is often stored in software with password protection; alternatively, the private key can be stored in a secure hardware token that prevents direct access or tampering.

There are key management problems associated with both symmetric-key cryptography and public-key cryptography. Symmetric-key cryptography schemes provide message confidentiality by requiring the sender and receiver to share a common, secret key. Each user must trust the other not to divulge the common key to a third party. They pose significant key management problems in networks of more than a very small number of users. If confidentiality is

compromised it becomes increasingly difficult to determine the point of compromise with a greater number of users. Public-key cryptography schemes require each party to have a key pair: a private key, which must not be disclosed to another user, and a public key, which may be made available in a public directory. Problems here arise with the availability of the public directory and maintenance of the public directory. One must ask: Is the public directory current and does it have the public key that is required?

Public-key systems simplify the key management problems associated with symmetric-key encryption; however, even more importantly, public-key cryptography offers the ability to efficiently implement digital signatures.

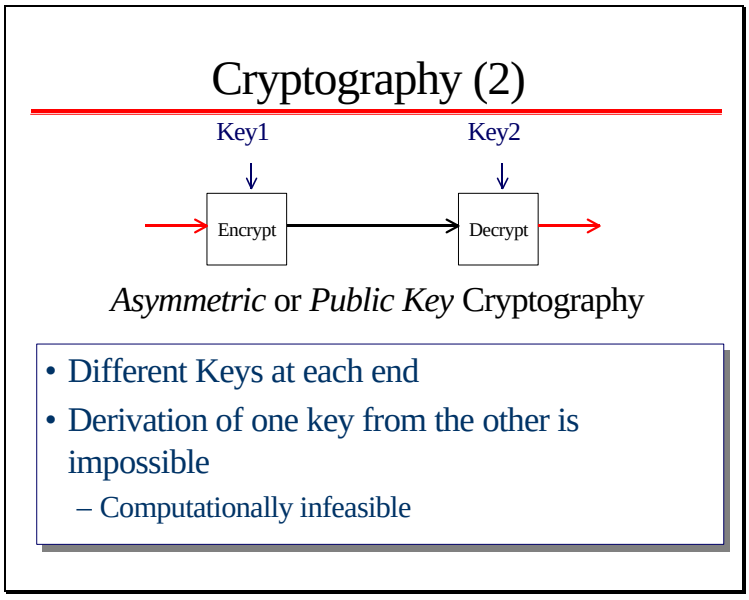

Figure 2. Public Key Cryptography

D. CONFIDENTIALITY, AUTHENTICATION INTEGRITY AND NON-REPUDIATION

Public key cryptography schemes provide mechanisms supporting confidentiality, authenticity, integrity and non-repudiation for the network and will now be described.

1. Confidentiality

Confidentiality is sometimes called secrecy or privacy. It involves keeping a message or data private. Typically it is provided by encryption.

2. Integrity

It is a measure of the state of wholeness or goodness of the resource or the degree to which it is accurate, complete, genuine, and reliable [Ref 21, p.25]. Typically it is provided by digital signatures in such a way that a message or data is not alterable without detection

3. Authentication

Authentication refers to mechanisms for confirming the identity of people, systems or information. Mechanisms include passwords, access tokens, biometrics, watermarks, and in networked environments digital signatures. They ensure that the quality or condition of information is authentic, trustworthy, and genuine and that users or senders of information are who they claim to be. Authenticity is typically provided by digital signatures.

The DoD PKI digital signature has been evaluated by the General Accounting Office as meeting the requirements to be legally binding electronic substitute for a "wet signature" on documents [Ref 28, p.1].

4. Non-repudiation

Non-repudiation means that a person cannot deny having sent or processed information. It is typically implemented by requiring the sender to digitally sign the information. At a later time a judge or a third party can establish that the sender really did send a message.

E. PUBLIC KEY INFRASTRUCTURE

A PKI encompasses "Certificate Management" and "Registration" functions and "Public Key enabled applications".

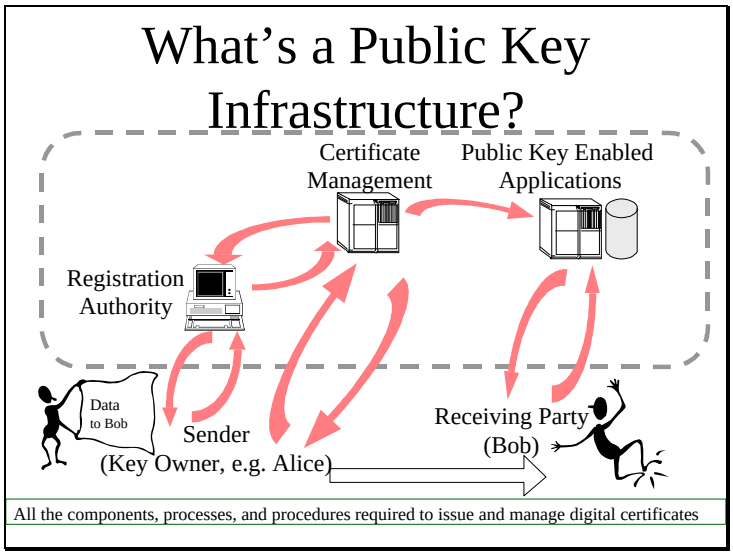

Figure 3. What's a Public Key Infrastructure?

1. Certificate Management

Certificates, similar to identification cards, are electronic credentials that are used to certify the online identities of individuals, organizations, and computers. Certificates are issued and certified by CAs. A certificate signed by a trusted third party binds an individual's public key to the individual. Thus we trust that any use of the public key in essence speaks for its owner.

Certificate Management provides for the generation, production, distribution, control, accounting and destruction for public key and public key certificates. Certificate Management is composed of a Certificate Authority (CA) and Directory Services. The CA plays the role of a trusted third party that certifies the identity of the possessor of a private key used for digital signature or key exchange by providing digitally signed certificates for users and components. Certificate management will also provide key recovery for private keys associated with encryption certificates to support data recovery.

Information contained in the certificate includes a version number, the issuer's name, a serial number, the individual or entity's name, public key, validity period for use and optionally other attributes or privileges [Ref 24,

Section 8, p.21]. The certificate management process in the DoD PKI will be responsible for:

> Digitally signing each certificate, thereby certifying the identity of the end entity possessing the corresponding private key.
>
> Managing the revocation of certificates. Two methods will be used to manage the revocation of certificates: (1) Publishing and posting a Certificate Revocation List (CRL) to the directory, and (2) Providing a mechanism for a real-time check of the revocation.
>
> Archiving all certificates and CRL's even after expiration or revocation, to support non-repudiation of digital signatures.
>
> Provide tools and procedures for personnel responsible for user registration status [Ref 1, p. 2,3].

To ensure consistent, proper usage of different assurance levels across the DoD, PKI certificates will be issued with assurance levels in accordance with the minimum criteria listed below:

> **Class 2**: (Formerly Basic) This level is intended for applications handling information of low value (Unclassified) or protection of system high information in a low to medium risk environment such as SIPRNET. This assurance level does not require that the end user register in person and their cryptography can be software based. Note: DoD will use Class 3 certificates to support Class 2 applications.
>
> **Class 3:** (Formerly Medium) This level is intended for applications handling medium value information in a low medium risk environment. This assurance level is appropriate for applications that typically require identification of an entity as a legal person, rather than merely as a member of an organization. This assurance level requires that the end user register in person and their cryptography can be software based.
>
> **Class 4:** (Formerly High) This level is intended for applications handling medium to high value information in any environment. These applications typically require identification of an entity as a legal person, rather than merely a member of an organization. This level requires a hardware token for protection of the private key material.

This assurance level requires that the end user register in person, and that the cryptography be hardware based.

Class 5: This level is intended for applications handling classified information in a high-risk environment (over an open unprotected network). This assurance level requires National Security Agency (NSA)-approved Type I cryptography [Ref 1, Appendix c-1].

To achieve interoperability of certificates across all DoD components, the DoD Class 3 identity and encryption certificates will have a minimum/common set of attributes (i.e. citizenship, government/non-government employee, service, or agency affiliation) [Ref 1, p. 2]. Interoperability between DoD and its vendors and contractors will be accomplished, in the near term, by using External Certification Authorities (ECAs).

Primarily CA Directory Services are used to distribute certificates and CRLs to users and applications. In addition, directories can be used to distribute other end-entity information such as e-mail address, phone numbers, postal address, etc. A directory system must be viewed from at least two perspectives: user access and administration. User access includes the suite of access protocols, as well as the means of controlling access to information within that repository. Also the directory system should be configured to use digital signatures for strong identification and authentication (I&A) as well as non-repudiation, of administrator actions.

2. Registration

Although the CA is ultimately responsible for identification and authentication during the certificate creation process, the CA may assign some of the responsibility to the Registration Authority (RA) and Local Registration Authority (LRA). In general the RAs/LRAs are responsible for authenticating the identity of users and entities during the creation of certificates. Certificates may also contain additional information and it is the responsibility of the RA/LRA to verify the accuracy of this information. The requirements for the RA/LRAs and associated tools are defined in the US DoD X.509 Certificate Policy [Ref 1, p.3].

Registration will be done through a workstation and web-based application. Hardware tokens will be used to help establish assurance of the process. A registration workstation with standardized procedures for the request and delivery of certificates will be based on commercial standards and technologies. A desired goal is a common set of processes and tools that supports certificate registration at all levels of assurance. The only difference in the registration process being user identification procedures and tokens used to protect the

keys. This will allow all users to register with the appropriate CA server through an LRA.

3. Applications and Standards

A PKI supports the employment of cryptographic security services by providing public key information, certificates and Certificate Revocation Lists (CRLs) to cryptographic applications, which encrypt and decrypt data and sign and verify signatures. To use public key technology, application developers must understand the supporting infrastructure's policies, usage and interfaces. There are a number of commercial off the shelf applications available today that use PKI certificates. Because of the newness of the standards and products, however, there can be some functional and interoperability problems between vendors' products. The Defense Information Systems Agency (DISA) and National Security Agency (NSA) are actively working with the vendors and the standards communities to achieve standard specifications and product implementations to ensure interoperability. The DoD is committed to ensuring that these DoD specifications are consistent with emerging commercial and National Institute of Science and Technology (NIST) Federal standards to support DoD interoperability requirements [Ref 1, p. 3]. The DoD PKI will also continue to track new and evolving Internet Engineering Task Force

(IETF) standards to ensure that the most widely accepted commercial standards are fully leveraged to support maximum interoperability in the future.

4. Biometrics

Security is enhanced by using multi-factored authentication. Commonly used factors are: something you know, something you have, something you are, and something you do. Password-based systems typically use only the first factor, i.e. something you know. A token adds an additional factor, and represents something you have. Two factor authentication has proven to be much more effective than single factor because the something you know factor is so easily compromised or shared. Biometric identification adds another factor providing something you are. Biometrics is the technology of measuring and statistically analyzing human body characteristics. Biometric identification can be classified into two groups: static biometric and dynamic identification.

Static biometric identification captures and verifies physiological characteristics of an individual. Common static biometric characteristics include fingerprints, eye retina, and facial features.

Dynamic biometric identification uses behavioral characteristics of an individual. Common dynamic biometric characteristics include voice and handwriting.

Biometric authentication requires readers or scanning devices, software that converts scanned information into digital form, and, wherever the data is to be analyzed, a directory that stores the biometric data for comparison with entered data. When converting a biometric input, the software identifies specific points of data as match points. The points are processed using an algorithm into a value that can be compared with the stored biometric value when a user tries to gain to access.

A smartcard token can be enhanced to include the something you are factor. Prototype designs are available, which use thumbprint biometrics from the thumbprint reader on the surface of the token in addition to the PIN in order to unlock the services of the token. Alternatively, a thumbprint biometric value, a retinal biometric value, or other biometric information can be stored on the card, which is checked against data obtained from a separate biometric input device. Similarly, Something you do such as typing patterns, handwritten signature characteristics, or voice inflection biometric values can be stored on the token and

be matched against data accepted from external input devices.

If the system is designed to allow for graded authentication, the administrator can assign different security labels based on the number and type of login factors deemed necessary to enable access to the requested data or services. For example variations include, Token only, Password only, Biometric only, Password and Token, Biometric and Token, Biometric and Password, and Biometric with password and Token.

F. CONCLUSION

This chapter introduced public key cryptography and gave a brief overview of what is required of a public key infrastructure. It covered utilization of public key cryptography to achieve confidentiality, authentication, integrity, and non-repudiation. Different assurance levels across DoD PKI certificates were introduced for future reference. A brief overview of how PKI will be implemented within the USMC will be provided in Chapter III.

III. USMC PKI IMPLEMENTATION

A. INTRODUCTION

Soon, nearly every Marine and DoD employee will need PKI services to support tactical users and daily activities. These services are becoming increasingly important in networked environments where communications and transactions occur over unsecured channels. The need for confidentiality, integrity and digital signatures can be provided by cryptography, which in turn needs the support of a PKI. In this chapter specific details of the PKI pertinent to the USMC will be discussed.

B. USMC PKI HIERARCHICAL STRUCTURE

The USMC PKI builds on the DoD PKI and consists of six entities in a top down hierarchical structure beginning with the Root Authority housed at the National Security Agency (NSA), Finksburg, MD.

1. Root Authority

The National Security Agency (NSA) will initialize and operate the Root Authority. The Root Authority will register and certify all DoD Certificate Authorities (CA). If the root CA is compromised then the integrity and security offered by the systems it supports is lost. The

root authority is not involved in daily functions of the PKI system.

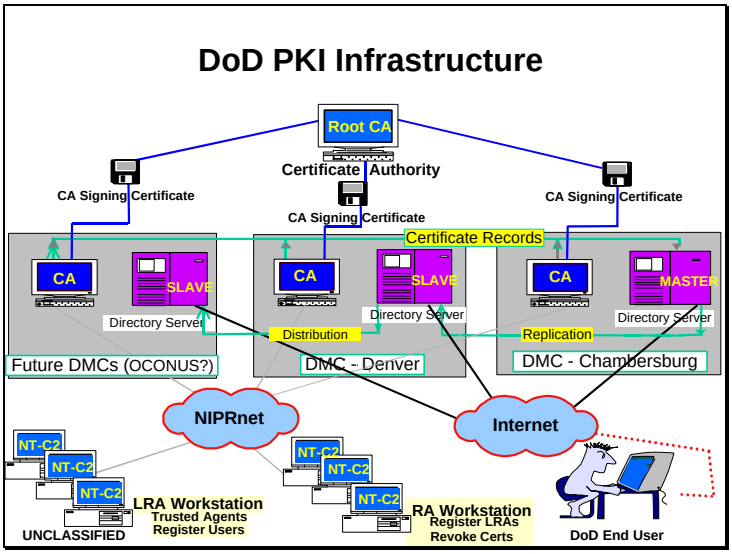

Figure 4. DoD PKI Infrastructure

2. Certificate Authority (CA)

The Defense Information Systems Agency (DISA) has been designated as the DoD, (e.g., USMC), Certificate Authority (CA). DISA will have at least four CA sites. Currently, there are two CAs. One CA is located at Defense Mega Center (DMC) Chambersburg, PA and the other resides at DMC Denver, CO. Two yet to be determined overseas sites, one in Europe and another in the Pacific are planned. These CAs are connected to the NIPRNET. A second set of CAs will be connected to the SIPRNET.

As the DoD CA, DISA will be the sole authenticator for the USMC Registration Authorities (RAs) and provide directory and certificate services and system management. The CA itself may generate some certificate information; but in general the CA is responsible for collecting information from authorized sources and correctly entering that information into a to-be-signed certificate. The CA is bound by its Certificate Practice Statement (CPS) to include only valid and appropriate information, and to maintain that due process is exercised in confirming the information.

3. Registration Authority (RA)

The USMC Registration Authority (RA) is the Marine Corps Information Technology Network Operation Center (MITNOC) Chief Information Officer (CIO). The MITNOC CIO will oversee the implementation of the USMC PKI. The USMC RA will register all USMC Local Registration Authorities (LRAs), servers, and maintain/submit certificate revocation lists (CRLs) to the CA. The RA will make the initial distribution of End-User certificates during the implementation of PKI. The RA will use the RA workstation to interact with the CA and will use a token reader and token for system access. The RA will manage LRA groups and LRA certificates. The RA also issues server certificates. The purpose of a server certificate is to act as an identity

certificate for server authentication when establishing a Secure Socket Layer (SSL) session.

4. Local Registration Authority (LRA)

Local Registration Authority's are local entities that identify and authenticate End-Users and register them as part of the certificate issuance process. LRAs will be designated in accordance with the USMC Network regionalization concept, where eight regions are currently being identified. Unit Commanders within each region will designate Information Systems Security Officers (ISSOs) within their region to act as the LRA. Custom software has been developed to provide a graphical user interface (GUI) for the LRA. This workstation and a web browser are used to register users during the certificate issuance process. The LRA workstation provides tools for creating lists of users, assigning unique identifiers (UID) and creating One-Time Passwords (OTP), which are needed by users to complete the certificate issuing process. The LRA workstation provides secure mechanisms for delivering the user lists to the CA server. These mechanisms include: file upload that uses a mode of the Secure Socket Layer (SSL) protocol that authenticates both the client and server system. LRAs also have the capability to reset users' login OTP, should the user fail to login properly after three attempts with the

OTP when trying to complete the certificate issuance process. LRAs are required to use token readers and tokens to access the system.

5. Trusted Agents (TA)

Trusted Agents (TAs) are local entities that verify end-users personal data, and perform face-to-face authentication. Trusted Agents assist RAs and LRAs when it is not geographically feasible for End-Users to physically come to an RA or LRA location. Unit Commanders within each region will designate Information System Security Officers (ISSOs) within their region to act as Trusted Agents on an as needed basis during and after the implementation of PKI.

6. End-Users

End-Users will use the USMC PKI in their daily duties, digitally signing and encrypting messages in support of various USMC functions. The End-User is responsible for interacting with the LRA for obtaining and maintaining personal certificates.

C. USMC PKI OBJECTIVES

Marine Corps networks support a variety of the Marine Corps' departmental and enterprise-wide applications. Several emerging joint applications are being developed and fielded with integrated public key mechanisms and PKI

interfaces. Examples include Electronic Document Access (EDA), Defense Travel Systems (DTS), Medium Grade Services (MGS), Navy Marine Corps Intranet (NMCI), and Joint Computer Aided Acquisition Logistical Support (JCALS).

DoD PKI policies are established at three fundamental levels: the entire DoD, the DoN (including the Marine Corps), and locally at the command level. DoD policies are the highest level of policies affecting the entire PKI and are the broadest of all policies. DoD policies are not designed to cover every detail of implementing a PKI. DoN and local policies cannot conflict with the overall DoD guidance, only enhance the overarching DoD policy. One of the more influential policy documents affecting DoD policy on PKI is Public Key Infrastructure Roadmap for the Department of Defense Version 2.0, Revision C, 08 September 2000. It states numerous dates for the implementation and deployment of the DoD PKI.

> DoD must deploy an infrastructure capable of issuing Class 3 DoD PKI certificates to each member of the organization by October 2000 [December 2001].
>
> All DoD users will, at a minimum, be issued a Class 3 PKI certificate by October 2001 [October 2002].
>
> To accelerate improved protection of information exchanged within the DoD, all e-mail sent within the DoD will be digitally signed by October 2001 [October 2002].
>
> DoD Components will begin to issue Class 4 certificates (on hardware tokens) in replacement of Class 3 certificates (software based) by January 2002 [October 2002].

> Systems using PKI technology to protect SBU information over unencrypted networks, such as e-mail, must migrate to the use of Class 4 certificates and hardware tokens by 31 December 2002 [December 2003].

The dates in brackets are the new DoD PKI Milestones approved 12 August 2000. With the timetable already established the Marine Corps must aggressively pursue its PKI implementation plan, strictly adhering to the established DoD PKI standards, to meet the objectives set forth in the above policies.

D. CONCLUSION

This chapter described the Marine Corps' role within the DoD's policies and overall strategy for PKI implementation. The USMC PKI Hierarchical Structure was explained. Marine Corps specific responsibilities and objectives for the implementation of a PKI within the USMC were presented and discussed. How tactical issues affect Marine PKI implementation will be discussed in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TACTICAL ISSUES AND PROPOSED SOLUTIONS

A number of focus groups were held between August 1999 and January 2000 to gather user requirements for both the Target Key Management Infrastructure (KMI) and DoD PKI. As a result of those focus groups, two requirements documents were produced.

- *Future KMI Operational Requirements Document* (Initial Draft), 29 October 1999
- *DoD Public Key Infrastructure User Requirements,* 29 February 2000

The goal of the focus group that met 7-8 June 2000 was to gather feedback on the contents of these two documents, and capture additional requirements that are not currently included in either of these documents. An area of particular interest for feedback on the PKI User Requirements document was Tactical PKI Requirements. From the results of that focus group, (Reference 18), some issues of concern included: Personnel, Physical Security, Hardware and Software, Transportation, Biometrics, Key Escrow/Recovery, Directories, Certificate Revocation List, Management of Tokens, Loss or Capture of Personnel and Equipment. For the remainder of the Chapter, I will define

the issues more deeply and give what I believe to be workable solutions to these issues.

A. TACTICAL PKI REQUIREMENTS

To understand the tactical PKI challenge, one must appreciate the basic definition of a tactical PKI. For purposes of this document, a tactical PKI is defined as “a PKI in support of combat operations”.

In the tactical environment, a tactical community should be able to replicate portions of the directory that are needed for a specific tactical operation without having to depend on the availability or reachback to the primary directories [Ref 18, #177]. In Chapter III the definition of a Certification Authority (CA) and Local Registration Authority (LRA) were given. A major difference between the two is that the CA is responsible for all aspects of the certificate issuance and management process. The LRA is a local registration agent that verifies end users and registers them prior to certificate issuance. If an LRA is deployed with enough pregenerated certificates and is held responsible for all aspects of the certificate issuance and management process it should be upgraded to a local tactical CA. This would allow for all the functions of the CA to

take place locally and not rely on reachback to the primary directories.

While the USMC PKI can support most tactical requirements through the use of a local tactical CA, there are still some issues concerning the completeness of the services provided by the local tactical servers. Since the tactical environment does not always provide easy access to the infrastructure elements (i.e., CA Servers, directory), services requiring such access may suffer. The services that suffer may include rapid mobilization, rapid compromise recovery required by tactical operations, key recovery, and support for remote users.

A tactical PKI includes the personnel and processes to perform PKI functions that include all processes including the availability of LRA personnel, the availability of tokens, etc. The tactical PKI should not inhibit the rapid mobilization of tactical communications and information systems. It should not degrade communications and should minimize bandwidth consumption as part of its basic design. It should support the rapid addition and removal of public key certificates to enable rapidly changing user roles and privileges. In addition, the deployment of a tactical PKI necessitates the need for a token that must meet tactical environment constraints.

The local tactical CA and associated directories will be required to support combined/joint coalition operations. Certificate management services will need to be self-contained/supported on isolated C2 networks. Interoperability with Allied/Coalition and NATO systems is crucial [Ref 18, #146].

B. ISSUES CONCERNING PERSONNEL, PHYSICAL SECURITY, HARDWARE AND SOFTWARE, TRANSPORTATION AND BIOMETRICS

1. Personnel

Some tactical PKI personnel related concerns are: Will a tactical PKI result in a “Zero-add” of personnel to units? If it is not a “Zero-add”, then what are the additional personnel requirements? Do we need to redesignate personnel (i.e., Staff Sergeant to Warrant Officer) to maintain a “Zero-add” approach?

With the Total Force Structure locked in place the procurement of additional personnel is highly unlikely. The Marine Corps should look at initiating a program designed to train and retain personnel in the Information Technology field. Many Marines are trained to perform specific Information Technology jobs, but when it is time to reenlist they opt to exit the Marine Corps for greater pay and a higher quality of life.

As with other critical Military Occupation Speciliaties (MOS's) the Marine Corps needs to add an incentive for that Marine to continue with a career in the Marine Corps. One possible solution is to require a payback period in return for training in certain IT skills. Reenlistment bonuses, and annual bonuses should be reviewed as other possible incentive tools. An examination of current occupational field distributions should be reviewed for redundancy and duplication, upon elimination of redundancies an opportunity for personnel to take training and transfer to new duties should be provided. If the data is classified, the personnel operating the equipment will also require an appropriate level of security clearance. The system must be capable of being managed by personnel with a basic/minimum knowledge of Information Technology and PKI system training

Allowing a Sergeant or Staff Sergeant the opportunity for selection to Warrant Officer can help to maintain a "Zero-add" approach to personnel requirements. Also, adding an Information Technology Management Military Occupation Specialty (MOS) to the Limited Duty Officer (LDO) board much, like the Ordnance and Logistics Field has done, can help in retaining Marines for a full career.

2. Physical Security

Physical security protection is an important aspect of a PKI. PKI components need to be secured to preclude loss from theft of components and to safeguard the data. Handling classified equipment is not new to the Marine Corps. The physical security of classified PKI components can be maintained along side already existing classified items. Two-person integrity (TPI) can be implemented when securing and shipping equipment needed for the operation of a tactical PKI. The computer equipment designated as the primary workstation for the LRA will be kept within a secure area. The information contained on the LRA machine is considered sensitive but unclassified (SBU). The personnel, as mentioned above will be screened for the proper clearance required for the task assigned. Again, this is not new to the Marine Corps.

3. Hardware and Software

The hardware (HW) and Software (SW) for the LRAs and users should be well thought out and specifically designed for tactically deployed units. If it is deemed necessary to have tactical LRAs or a local tactical CA, serious consideration should be given to the workstation requirements. The readers and tokens should withstand a

host of environmental scenarios such as sand, heat, and humidity and should also be small and lightweight.

A medium assurance (Class 3) PKI LRA requires the following software: Windows NT 4.0, and NETSCAPE 4.05 or greater, (US version only), with NETSCAPE Communicator, and the Local Registration Authority (LRA) SW and Graphical User Interface (GUI) available from Director, Communications Security Material (DCMS).

A medium assurance (Class 3) PKI LRA requires the following hardware: Pentium PC, Token Reader, standalone printer, Tokens and when required Internet connectivity. End-Users require a PC with Windows NT 4.0, NETSCAPE 4.05 or greater with NETSCAPE Communicator and Internet connectivity. End-Users will require token readers after the migration to the medium and high assurance (Class 4) PKI that uses hardware based cryptographic tokens.

4. Transportation

The total tactical PKI system must be transit cased and have a 2-man lift maximum weight, 200 lbs [Ref 18, #161]. Transport requirements should address airlift and vehicle capabilities (i.e., roll-on or sling loaded).

Locking weatherproof cases need to be provided to transport all associated equipment as specified in subparagraph 3. Standard 9 cubic foot boxes can be utilized

or the owning unit can manufacture boxes. A standard case made out of plastic with shock resistant material lining inside would be preferable.

5. Biometrics

More biometrics needs to be implemented into the tactical PKI [Ref 18, #226]. The implementation of biometrics into a tactical PKI needs to be incorporated during this early stage of the development process.

There are many environmental concerns that need to be considered when implementing biometrics into the tactical environment. Sand, water, extremes in temperature are just a few. An implementation of biometrics for the tactical environment can be fingerprint match points stored on a token and in devices such as cell phones. The token does not need a fingerprint to operate. The cell phone with a fingerprint reader embedded at the base needs a match between what it reads with what is stored in its directory and what match points the token provides. In this case the cell phone can only be activated if there is a three way match between the points stored on the token with what is provided by the fingerprint reader and what is stored in the cell phone.

C. KEY ESCROW/RECOVERY AND DIRECTORIES

1. Key Escrow/Recovery

Key recovery systems work in a variety of ways. Early "key recovery" proposals relied on the storage of private keys by a trusted third party. Recently, techniques that use "escrow agents" or "key recovery agents" have been proposed. These systems build an encrypted copy of the "session key" that is stored with the data. The key used to encrypt the session key is only known to the recovery agent. Some systems split the ability to recover keys among several agents.

Key escrow/recovery supports a number of important services, such as a backup mechanism that ensures that a tactical component will continue to have access to its own encrypted archive in the event that a public or private key is lost. The system put in place should address the capability of rapid access to all current and previous encrypted data. It is not difficult to design and implement small-scale systems that successfully recover keys or plaintext according to some access policy. The difficulties arise from ensuring that a large-scale system, or system of systems, does not inadvertently or maliciously leak data. All key recovery systems require the existence of a highly sensitive and highly available secret key or collection of

keys that must be maintained in a secure manner over an extended time period. These systems must make decrypted information quickly accessible to the correct tactical component. These basic requirements make the problem of general key recovery difficult, expensive and potentially too insecure and too costly for many applications and many users.

The impact of key recovery can be considered in at least three dimensions: Risk, Complexity, and Economic Cost. Risk for a key recovery system deals with the failure of key recovery mechanisms that can jeopardize the proper operation, underlying confidentiality, and ultimate security of the encryption systems. Threats include improper disclosures of keys, theft of valuable key information, or failure to be able to meet tactical demands. A fully functional key recovery infrastructure is an extraordinarily complex system with numerous new entities, keys, tactical requirements, and interactions. The true economic cost of a key recovery infrastructure is difficult to model.

It is still possible to make sound judgments about the basic system elements, shared by all key recovery systems. Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature [Ref 12, p 18]. Key recovery

degrades many of the protections available from encryption, such as absolute control by the user over the means to decrypt data.

In spite of these difficulties key escrow and key recover services must be provided locally in tactical situations. A tactical component cannot rely on reachback to recover encryption private keys.

2. Directory Services

Directory services must be available/tailored to support the user community of the tactical network. Deployed tactical components require real-time support, and the occasional “down” CA or directory will degrade an operation’s effectiveness. Local tactical directories need to be self-contained, so that they do not need to rely on reachback for updates or replication. Two techniques can be employed to minimize directory size to conserve bandwidth during replication and updates. The first is to issue certificates on a one-to-many basis instead of on a 1-to-1 basis. Within a tactical component you may have three identical sub components with identical traits and characteristics that carry out the same tasks. If the only one of the sub components is used at a time, then you only need to issue certificates to the sub component conducting a tactical operation. The second is to replicate only the

part of the directory that is needed for a tactical operation. However, the local tactical CA should still have the same real-time capability for certificate revocation, key recovery and certificate status checking.

D. CERTIFICATE REVOCATION LIST (CRL)

Certification Practices Statements describe operational aspects of a PKI. They need to be tailored to specific environments. Depending on the nature of an operation or tactical scenario, differing procedures will need to be established regarding operations such as compromise notification/recovery, certificate revocation, certificate revocation delay (i.e., minimum acceptable time to post revocation to CRL or update Online Certificate Status Protocol services), and frequency of directory updates.

1. CRL Distribution Scheme

Certificate revocation is just as important in tactical situations as it is in non-tactical situations. Thus CRLs need to be maintained to support tactical network users. Currently, the DoD PKI uses X.509 version 3 (X.509v3) CRLs that have extension fields that can provide many advantages. X.509v3 certificates allow CAs to define the extension fields as they see fit. Extension fields may contain additional information that can be specified for optional

use within a PKI. One possible use for extension fields is to contain a CRL number. If each CRL issued for a given certificate population is assigned a sequentially increasing number, users can determine if they are missing a CRL. The extension fields can also be used to reduce the bandwidth required for updates of CRL information. One such technique uses the concept of Delta-CRLs.

Rather than issue a full CRL, the local tactical CA can simply issue a list of the changes that have occurred since the last time a full CRL was issued. Users who maintain their own CRL database can use a delta-CRL to keep their copies updated without having to download and process all the entries of a full CRL, saving bandwidth and computing time. An extension field in the CRL designates a CRL as either a full CRL or delta-CRL.

The extension fields also allow a “revocation reason” to be specified for each revoked certificate in a CRL. This field allows CRLs to be partitioned by revocation reason.

Routine revocations, for example, those due to name change or lost password, can be placed on a separate CRL from one listing certificates that have been revoked for security reasons. The list of routinely revoked certificates can be distributed less frequently without

affecting the possibility of using a compromised certificate.

CRLs can also be partitioned on a component basis. Thus if a user needs to verify the validity of a certificate of a user from a specific component, they only need to check the CRL from that specific component rather than the full CRL.

All of these CRL extensions still do not overcome the fundamental problem of a lag in time between when a certificate is compromised and when its revocation appears on an end users CRL. Even with partitioned CRLs and frequent delta-CRL issuance, there is still a window of opportunity when a compromised certificate could be used.

2. Emergency Revocation

The tactical PKI should have a provision for emergency revocation in case of overrun or capture which can be executed in a worst-case time of 15 minutes, with 5 minutes being the desired time [Ref 18, #149].

The decision to execute emergency revocation is predicated on the current tactical situation. If the tactical component commander believes that due to the current tactical situation that it would be in the best interest of the overall operation to revoke the certificates of the component, then there should be an efficient means to

do so. Situations may include but are not limited to, overrun by the enemy or the detection of a traitor in the component. The tactical component stranded without PKI credentials would have to rely on other types of cryptography when communicating until the current situation can be corrected.

It can be implemented efficiently if the certificates for each tactical component in a tactical operation are identified by their tactical component name. If this is done, all certificates for a tactical component can be revoked by just sending back a high priority message with just the name of the tactical component. By using just the name, bandwidth would be conserved.

E. MANAGEMENT OF TOKENS

1. Management of Tokens

Service members will perform jobs that will require the use of their PKI tokens. If they show up to perform their jobs and their token fails, how quickly can the infrastructure react to resolve the problem?

Tactical tokens should be issued and managed in the same manner that weapons are issued and managed. The local tactical CA should deploy with enough pregenerated certificates and corresponding tokens for all members of the

tactical component and some spares to prevent the need for reach back to CONUS. Marines who use PKI-enabled applications to conduct daily garrison business will use their garrison token. Marines in support of a tactical operation who are in need of a tactical token and certificate will be issued a sanitized tactical token on an as needed basis allowing the Marine to leave behind their garrison token.

The argument for a sanitized tactical token, which is different from the garrison token is based upon the fact that currently garrison tokens are intended to include DoD personnel information (medical/dental records, dependent information, etc.) in addition to PKI cryptographic data and processing [Ref 29, p.6]. It would be extremely unwise (and a departure from current practice) to carry this personal information into a tactical situation.

When a tactical operation is begins, the local tactical CA sends a message to the RA notifying it of certificates issued and the corresponding user identification associated with those certificates. When the operation ends the tokens will be turned in for storage and a message will be sent to the RA notifying it as to which tokens have been returned. Although the technology allows for more than one private key on a token, I believe that the use of distinct sanitized

tactical token should be issued if there is a risk that the garrison token may become comprised. Private encryption keys associated with deployable tactical accounts must be locally escrowed and the escrowed keys must be deployed to support in-theatre key recovery. The certificates/tokens associated with the tactical accounts will need to be revoked upon exercise/operation termination.

2. Types of Tokens

Before the Marine Corps commits to a Common Access Card (CAC) or other token for the tactical environment it needs to ensure that the tokens and readers can hold up under the various tactical conditions.

In non-tactical contexts, the token used to store a users private key is currently the CAC. A CAC is very similar to your VISA credit card. The magnetic stripe on the back allows digitized data to be stored on the card in a machine-readable format. The stripe’s storage capacity is about 1000 bits and anyone with the appropriate read/write device can view or alter the data. For increased protection and to make the client token more powerful, an integrated circuit was incorporated into the card and the integrated circuit card has now become known as the Smart Card. Smart cards are now available with over 20 Kbytes of memory. Smart cards have both pros and cons. There are concerns

with smart cards as to how well they will stand up to a host of environmental scenarios, such as sand and sea salt spray, common to Marine Corps tactical situations. Proper maintenance is required for both the smart card and the smart card reader. Recent exercises have proven that sand is an environmental hazard to smart card readers that can render them useless.

One alternative is a key-sized token that the individual can carry on a key ring and plugs into the USB port of the machine being used. CYLINK'S Minikey is an example of this type of token. It is no bigger than a vehicle key. The USB port can be covered with a rubber grommet when not in use. How well this will work with handheld devices, such as a Personal Digital Assistant (PDA) and cell phones, still needs to be addressed. One advantage of smart cards is their ability to store additional information, such as a bar code and a picture for increased authentication in addition to keys in support of the DoD PKI

F. LOSS OR CAPTURE OF PERSONNEL AND EQUIPMENT

1. Rapid Voiding of Memory

Tactical threats that must be accounted for include: overrun and capture, equipment destruction, loss of nodes of the network due to jamming, loss of personnel due to

causalities, etc. Thus all tactical equipment, cell phones, Personal Digital Assistant, and PKI tokens must support rapid voiding of memory in case of capture or must be constructed with self-destructing tamper proof technology.

This includes, a method for zeroizing the local tactical CA data (e.g. CA directory) that can be executed by a switch or a command sequence initiated by the administrator with the proper token.

2. Suspension of Credentials

There should be a capability for suspending certificates for individuals whose status has become unknown, and for reinstating the individual's certificates once active status has been confirmed.

The following scenario illustrates the need for this capability. Suppose an individual disappears behind enemy lines and later attempts to communicate with the tactical network. If the user's certificate has been revoked, this communication will be denied.

One way to support the capability of suspending/reinstating user's certificates is through the use of "revocation reason codes" in CRLs. Thus, a CRL can list the certificates that are currently suspended until proper notification that the certificate has been compromised. If a suspended certificate is used, the

message will still be accepted but it will be flagged as questionable.

G. CONCLUSION

This chapter has described some of the tactical issues that affect the Marine Corps' role, policies and overall strategy for a PKI implementation. Proposed solutions to the tactical effects were discussed. A summary, conclusion and recommendations for further research will be discussed in Chapter V.

V. DISCUSSION AND CONCLUSIONS

A. DISCUSSION

The United States Marine Corps (USMC) Public Key Infrastructure (PKI) is defined as the framework and services that provide for the generation, production, distribution, control, and tracking of public key certificates. It is a major element of the Marine Corps Information Assurance (IA) strategy that is based on a "Defense-in-Depth" concept.

At present, the DoD PKI program Management Office (PMO), in conjunction with the Defense Information Systems Agency (DISA), Federal agencies, and Services are working against an existing timeline to provide a standard PKI capability. Since the technology is still evolving, the Marine Corps hopes to influence current products with Marine Corps requirements by using a strategy of early participation with current vendors. This, in turn, should minimize the use of Government-Off-the-Shelf (GOTS) development and leverage existing commercial PKI technology, standards, and services.

Both the USMC Class 3 PKI and the target Class 4 PKI employ centralized certificate management and decentralized registration. Using this architecture, the USMC will issue

certificates to all it members, to include USMC (DoD) civilian personnel, by October 2002. However, the tactical environments that the military faces present a unique set of challenges to this architectural approach. Since the current DoD PKI was not designed with the tactical environment in mind, the full extent of deficient operation in the field is unknown. The nature of the tactical arena invariably suggests that the USMC must employ alternative solutions, at least in part, to institute a PKI tactically. The challenge, in part arises from the need to alter the architecture to fit the requirements of the tactical arena. Based on experience and technical knowledge, the USMC has identified areas of concern, which was the focus of this document.

The Marine Corps is ideally suited for joint, allied, and coalition warfare. It is the only Service specifically tasked by Congress to operate as an integrated combined arms force providing a joint force enabler in three dimensions—air, land, and sea. The Marine Corps operates as part of a larger joint force. Marine Corps Strategy 21 [Ref. 21] guides a Marine Corps capable of accomplishing its specified and implied tasks derived from the guidance in the National Security Strategy, the National Military Strategy, and other strategic documents. Marine Corps Strategy 21 also supports

Joint Vision 2020, which builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing evolution of the Armed Forces. Marines must analyze and influence this evolution.

As first described in Joint Vision 2010, the potential of the information revolution will be used to transform today's capabilities for maneuver, strike, logistics, and protection to become dominant maneuver, precision engagement, focused logistics, and full dimensional protection. To build the most effective force for 2020, we must be fully joint: intellectually, operationally, organizationally, doctrinally, and technically [Ref 26, p. 2].

Three aspects of the world of 2020 have significant implications for the US Armed Forces:

> First, the United States will continue to have global interests and be engaged with a variety of regional actors.
>
> Second, potential adversaries will have access to the global commercial industrial base and much of the same technology as the US military.
>
> Third, we should expect potential adversaries to adapt as our capabilities evolve [Ref 26, p. 5,6].

A difference between Joint Vision 2010 and Joint Vision 2020 is the addition of the term full spectrum dominance. The term full spectrum dominance implies that US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific

situations and with access to and freedom to operate in all domains—space, sea, land, air, and information [Ref 26, p. 8]. Upon realizing the potential of the information revolution, the transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation.

Joint Pub 1-02 contains the following two definitions:

> **Information environment**–the aggregate of individuals, organizations, and systems that collect, process, or disseminate information, including the information itself.
>
> **Information superiority**–the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information, information processing, and communications networks are at the core of every military activity.

B. CONCLUSIONS

Addressing the requirements for the deployment of a PKI in the USMC tactical environment is a difficult and ongoing task. As mentioned earlier, the USMC is ideally suited for joint, allied, and coalition warfare. It is the only Service specifically tasked by Congress to operate as an integrated combined arms force providing a joint force enabler in three dimensions: air, land, and sea. The Marine Corps operates as part of a larger joint force. Operation in a Joint environment imposes additional requirements

regarding the of commonality of equipment and applications to support a tactical PKI.

A PKI Pilot for Tactical USMC needs to be conducted. The purpose of the Pilot should be to deploy Public Key Technology to understand operational benefits and shortfalls. The pilot program will allow leveraging of cryptographically supported commercial security technology where applicable. It will also facilitate the development, integration and testing of Government off the Shelf (GOTS) cryptographically supported security technology to meet specific USMC tactical requirements. To produce useful results, any worthwhile pilot would have to be conducted in a coalition network/environment. A pilot program will also allow the USMC to validate current solutions envisioned for the tactical arena. The USMC needs to continue work on a tactical PKI Operational Requirements Document (ORD), separately from the DoD PKI ORD, so that USMC specific requirements can be met.

The USMC needs to establish and coordinate tactical PKI forums and workshops. Also the USMC should not plan in a vacuum. Looking outside to other services and to the private sector can assist in the search for a workable solution. It is important to realize that each of the Services' specific missions and roles will create different

definitions of “tactical”. Of course, the nontactical PKI and the tactical PKI, will have to interoperate.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

Below are some recommendations for future research:

1) Some tactical networks are on the SIPRNET, and some are not. There should be some research into the requirements for tactical/deployed unit’s networks (i.e., SIPRNET).

2) Identify and discuss the full impact on privacy and security of using a DoD Common Access Card. For example, given that the future military ID card will be a smart card containing PKI certificates, what are the possible implications and risks? What information should/should not be contained on the smart card?

3) Which weapons systems/applications are candidates for PK enabling (i.e., require PKI services of authentication, integrity, non-repudiation, confidentiality, or availability)? For example, would existing artillery/call for fire systems benefit from the additional authentication/data integrity mechanisms provided via PKI digital certificates? What are the disadvantages? Would implementing a PKI increase the length of time that it takes to request support from a call for fire system? Would

implementing a PKI degrade the Quality of Service of a call for fire system or enhance it?

4) Systems using PKI technology to protect SBU information over unencrypted networks, such as e-mail, must migrate to the use of Class 4 certificates and hardware tokens by 31 December 2002. Given this deadline, what standard token should be used? Smart Cards are currently being discussed, but with the increasing varieties of Smart Cards what standards (i.e., power currently 5 volts, mobile phone components currently 3 volt) are to be adhered to?

D. SUMMARY

This thesis has identified and described a few of the issues challenging the deployment of a PKI in the USMC tactical environment. Some of the issues will be overcome with the use of a well thought-out and robust tactical token. Also, the use of CRL extensions will help maintain current and efficient certificate directories. Equipment self-protection will also aid in assuring security. The development of a solution for the tactical arena is a fluid and complex challenge that needs to be addressed in order to ensure the best support of tactically deployed forces.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. ABBREVATIONS AND ACRONYMS

ASD	Assistant Secretary of Defense
C2	Command and Control
C3I	Command, Control, Communications and Intelligence
CA	Certificate Authority
CAC	Common Access Card
CIO	Chief Information Officer
CPS	Certificate Practice Statements
CRL	Certificate Revocation List
DISA	Defense Information System Agency
DII	Defense Information Infrastructure
DMC	Defense Mega Center
DMS	Defense Message System
DoD	Department of Defense
DoN	Department of the Navy
DTS	Defense Travel System
EDA	Electronic Document Access
GOTS	Governments off the Shelf
GUI	Graphic User Interface
IA	Information Assurance

I&A	Identification and Authentication
ISSO	Information System Security Officer
JCALS	Joint Computer Aided Acquisition Logistical Support
KMI	Key Management Infrastructure
LDO	Limited Duty Officer
LRA	Local Registration Authority
MOS	Military Occupation Specialty
MGS	Medium Grade Service
MITNOC	Marine Corps Information Technology Network Operation Center
NIPRNET	Nonclassified Internet Protocol Routing Network
NMCI	Navy Marine Corps Intranet
NSA	National Security Agency
ORD	Operational Requirements Document
OTP	One Time Password
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
RA	Registration Authority
S/MIME	Secure Multipurpose Internet Mail Extension

SBU	Sensitive But Unclassified
SIPRNET	Secret Internet Protocol Routing Network
SSL	Secure Socket Layer
TA	Trusted Agent
UID	Unique Identifiers
US	United States
USMC	United States Marine Corps

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. DOD Public Key Infrastructure Program Management Office, *Public Key Infrastructure Roadmap for the Department of Defense* Version 2.0*,* Revision C, 08 September 2000.

2. DOD Public Key Infrastructure Program Management Office, *DOD Certificate Policy Version 5.0*, 13 December 1999.

3. Deputy Secretary of Defense, *Memorandum Subject: Department of Defense (DoD) Public Key Infrastructure (PKI)*, 6 May 1999.

4. Hackerson, J.X., "Rethinking Department of Defense Public Key Infrastructure" paper presented at the 23rd National Information Systems Security Conference, Baltimore, Maryland, 17 October 2000.

5. Morris, D.E. and Rowe, D.W., *Preliminary Roadmap for the United States Marine Corps Public Key Infrastructure,* Master's Thesis, Naval Postgraduate School, Monterey California, September 1999.

6. Berkovits, S., Chokhani, S., Furlong, J.A., Geiter, J.A., and Guild, J.C., *Public Key Infrastructure Study: Final Report,* Produced by the MITRE Corporation for NIST, April 1994.

7. Cooer, D.A., "A more efficient use of Delta-CRL's (Draft)" Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD, 20899-8930, 25 October 1999.

8. DOD Public Key Infrastructure Program Management Office, *DOD Public Key Infrastructure Roadmap*, Version 1.0, 11 August 1998.

9. Booz, Allen & Hamilton Inc., *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*, 4 January 1999.

10. United States Marine Corps, *Class 3 Certificate (Medium Assurance) Public Key Infrastructure (PKI)*, Draft Guidance, 15 March 1999.

11. Department of the Navy, *Medium Assurance (Class 3) Public Key Infrastructure (PKI)*, Draft Guidance, 21 April 1999.

12. Abelson, H., and others, *The RISKS of Key Recovery, Key Escrow, & Trusted Third Party* Encryption, Digital Issues no. 3, June 1998.

13. Department of Defense, *Target Public Key Infrastructure User* Requirements, 29 February 2000.

14. Federal Card Services Task Force Electronic Process Initiatives Committee, *Federal Smart Card Implementation Plan*, 30 January 1998.

15. DOD Public Key Infrastructure Program Management Office, *Future KMI Operational Requirements* Documents, Initial Draft, 22 October 1999.

16. Novell, *Other Methods of Authentication Supported by NMAS, Physical Device Authentication*, March 2000. [http://developer.novell.com/research/devnotes/2000/march/03/d0003033.htm].

17. DOD Public Key Infrastructure Program Management Office, *Certification Practices Statement for the Certificate Management Infrastructure of the Defense Information Infrastructure*, Draft, Version 0.2, 10 April 1998.

18. PKI Tactical Functional Requirements ORD Development Workshop, *PKI User Requirements Assessment Document*, 7-8 June 2000.

19. Petri, S., Litronic, Inc., *An Introduction to* Smart cards, [http://www.litronic.com/whitepaper/index.html]. 13 September 2000.

20. NIST PKI Project Team, *Certificate Issuing and Management Components; Protection Profile,* Draft, 5 May 2000.

21. Denning, Dorothy E., *Information Warfare and Security*, Addison Wesley Longman, Inc., 1999.

22. Pfleeger, Charles P., *Security in Computing*, Prentice-Hall P T R, 1996.

23. DoD Chief Information Officer, Assistant Secretary of Defense, *Department of Defense (DoD) Public Key Infrastructure (PKI)*, Memorandum, 12 August 2000.

24. Naval Postgraduate School Center for Information Systems Security Studies and Research, *Introduction to Computer Security course notes and documentation*, Spring 2000, 1998.

25. Booz,Allen & Hamilton Inc., Technical Task Order 442, *DoD Tactical PKI Planning Document*, Draft, Version 2.1, Booz,Allen & Hamilton Inc., 16 January 2001.

26. Director for Strategic Plans and Policy, J5; Strategy Division, *JOINT VISION 2020*, US Government Printing Office, Washington DC, June 2000.

27. Department of the Navy, Headquarters United States Marine Corps, *Marine Corps Strategy 21*, US Government Printing Office, Washington, DC, 3 November 2000.

28. Department of Defense, *PKI Reporting and Escrow Requirements*, Draft, 20 November 1998.

29. United States Marine Corps, *Nonclassified Internet Protocol Routing Network, Public Key Infrastructure, Concept of Operations*, 13 March 2001

30. Assistant Secretary of Defense, *Memorandum Subject: Smart Card Adoption and Implementation*, 10 November 1999.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center.....2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library.....2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5000

3. Professor Cynthia E. Irvine, Code CS/Ic.....2
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943-5118

4. Professor Daniel F. Warren, Code CS/Wd.....1
   Department of Computer Science
   Naval Postgraduate School
   Monterey, CA 93943-5118

5. Director, Training and Education.....1
   MCCDC, Code C64
   1019 Elliot Road
   Quantico, VA 22134-5107

6. Director, Marine Corps Research Center.....2
   MCCDC, Code C40RC
   2040 Broadway Street
   Quantico VA 22134-5107

7. Marine Corps Representative.....1
   Naval Postgraduate School
   Code 037, Bldg.330, Ingersoll Hall, Room 116
   555 Dyer Road
   Monterey, CA 93943

8. Marine Corps Tactical Systems Support Activity.....1
   Technical Advisory Branch
   Attn: Librarian
   Box 555171
   Camp Pendleton, CA 92055-5080

9. Carl Siel.....1
Space and Naval Warfare Systems Command
PMW 161
Building OT-1, Room 1024
4301 Pacific Highway
San Diego, CA 92110-3127

10. Major Dan Morris.....1
HQMC
C4IA Branch
To: Navy Annex
Washington DC 20380

11. Commander, Naval Security Group Command.....1
Naval Security Group Headquarters
9800 Savage Road
Suite 6585
Fort Mead, MD 20755-6585

12. Ms Louise Davidson.....1
N643
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202

13. Capt. James Newman.....1
N64
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202

14. Mr. Richard Hale.....1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

15. Ms. Barbara Flemming.....1
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230

16. Major Alan R. Stocks.....1
40 Tavern Road
Stafford VA, 22554